CLAIMS

1. An authentication communication system which includes (a) a storage medium having an area for storing digital information and (b) an access device for reading/writing digital information from/into the area, the authentication communication system comprising:

a first authentication phase in which the access device authenticates whether the storage medium is authorized according to a challenge-response authentication protocol by transmitting scrambled access information generated by scrambling access information which shows the area, to the storage medium;

a second authentication phase in which the storage medium authenticates whether the access device is authorized; and

a transfer phase in which, when the storage medium and the access device have authenticated each other as authorized devices, the storage medium extracts the access information from the scrambled access information, and the access device reads/writes digital information from/into the area shown by the access information.

2. The authentication communication system of Claim 1,

wherein in the first authentication phase,

the access device includes:

an access information acquisition unit for acquiring

the access information which shows the area;

a random number acquisition unit for acquiring a random number;

a generation unit for generating random number access information by combining the access information and the random number; and

an encryption unit for encrypting the random number access information according to an encryption algorithm, to generate the scrambled access information,

the storage medium includes a response value generation unit for generating a response value from the scrambled access information, and

the access device includes an authentication unit for authenticating whether the storage medium is authorized using the response value.

3. The authentication communication system of Claim 2,

wherein in the transfer phase, the storage medium includes:

a decryption unit for decrypting the scrambled access information according to a decryption algorithm to obtain the random number access information; and

a separation unit for separating the access information from the random number access information.

4. The authentication communication system of Claim 3,

wherein in the first authentication phase,

the access device further includes a random number seed storage unit for storing a random number seed, and

the random number acquisition unit acquires the random number by reading the random number seed from the random number seed storage unit.

5. The authentication communication system of Claim 4,

wherein in the first authentication phase, the access device further writes the scrambled access information over the random number seed stored in the random number seed storage unit, as a new random number seed.

6. The authentication communication system of Claim 3,

wherein in the first authentication phase,

the access device further includes a random number seed storage unit for storing a random number seed, and

the random number acquisition unit acquires the random number, by reading the random number seed from the random number seed storage unit and generating the random number based on the random number seed.

7. The authentication communication system of Claim 6,

wherein in the first authentication phase, the access device further writes the random number over the random number seed stored in the random number seed storage unit as a new random number seed.

8. The authentication communication system of Claim 3, wherein in the transfer phase,

the storage medium, which stores digital information in the area, includes an encryption unit for reading the digital information from the area shown by the access information and encrypting the digital information according to an encryption algorithm to generate encrypted digital information, and

the access device, which reads the digital information from the area, includes a decryption unit for decrypting the encrypted digital information according to a decryption algorithm to obtain the digital information, the decryption algorithm being an algorithm for decrypting a cryptogram generated according to the encryption algorithm.

9. The authentication communication system of Claim 3, wherein in the transfer phase,

the access device, which writes digital information into the area, includes:

a digital information acquisition unit for acquiring the digital information; and

an encryption unit for encrypting the digital information according to an encryption algorithm to generate encrypted digital information, and

the storage medium includes a decryption unit for decrypting the encrypted digital information according

to a decryption algorithm to obtain the digital information, and writing the digital information into the area shown by the access information, the decryption algorithm being an algorithm for decrypting a cryptogram generated according to the encryption algorithm.

10. The authentication communication system of Claim 3, wherein in the transfer phase,

the access device, which writes digital information into the area, includes:

a digital information acquisition unit for acquiring the digital information;

a content key acquisition unit for acquiring a content key;

a first encryption unit for encrypting the acquired content key according to a first encryption algorithm to generate an encrypted content key;

a second encryption unit for encrypting the encrypted content key according to a second encryption algorithm to generate a double-encrypted content key; and

a third encryption unit for encrypting the digital information according to a second encryption algorithm using the content key, to generate encrypted digital information,

the storage medium includes a decryption unit for decrypting the double-encrypted content key according to a first decryption algorithm to obtain the encrypted

content key, and writing the encrypted content key into the area shown by the access information, and

the storage medium further includes an area for storing the encrypted digital information.

11. An authentication communication method which includes (a) a storage medium having an area for storing digital information and (b) an access device for reading/writing digital information from/into the area, the authentication communication method comprising:

a first authentication step in which the access device authenticates whether the storage medium is authorized according to a challenge-response authentication protocol by transmitting scrambled access information generated by scrambling access information which shows the area, to the storage medium;

a second authentication step in which the storage medium authenticates whether the access device is authorized; and

a transfer step in which, when the storage medium and the access device have authenticated each other as authorized devices, the storage medium extracts the access information from the scrambled access information, and the access device reads/writes digital information from/into the area shown by the access information.

12. A computer-readable storage medium which stores an

authentication communication program for use in an authentication communication system (a) which includes a storage medium having an area for storing digital information and an access device for reading/writing digital information from/into the area, and (b) in which the digital information is transferred after each of the storage medium and the access device authenticates each other as authorized devices, the authentication communication program comprising:

a first authentication step in which the access device authenticates whether the storage medium is authorized according to a challenge-response authentication protocol by transmitting scrambled access information generated by scrambling access information which shows the area, to the storage medium;

a second authentication step in which the storage medium authenticates whether the access device is authorized; and

a transfer step in which, when the storage medium and the access device have authenticated each other as authorized devices, the storage medium extracts the access information from the scrambled access information, and the access device reads/writes digital information from/into the area shown by the access information.

13. An access device which is included in the authentication communication system of Claim 1.

14. An access device which is included in the authentication communication system of Claim 2.

15. A storage medium which is included in the authentication communication system of Claim 1.

16. A storage medium which is included in the authentication communication system of Claim 3.